Corrigé de l'épreuve XA

– 2020 –

Première partie

1. La matrice $A = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \in S_2(\mathbb{Q})$, son polynôme caracteristique est $X^2 - 2$. Donc $\pm\sqrt{2}$ sont des valeurs propres de A.

2. ..

   (a) Comme $\chi_M = X^2 - Tr(M)X + \det M$ et $M \in S_2(\mathbb{Q})$, alors $Tr(M), \det M$ sont dans $\mathbb{Q}$. Et Comme $\sqrt{3}$ est valeur propre de M, alors $\chi_M\left(\sqrt{3}\right) = 0$, donc $3 - Tr(M)\sqrt{3} + \det M = 0$. Donc $Tr(M)\sqrt{3} \in \mathbb{Q}$, et comme $\sqrt{3} \notin \mathbb{Q}$ et ce dernier est un corps, alors $Tr(M) = 0$ et par suite $\det M = -3$. Donc $\chi_M = X^2 - 3$

   (b) Si n est congru à 0 ou à 1 modulo 3, alors n^2 aussi, et si n est congru à 2 modulo 3, alors n^2 est congru à $2^2 = 3 + 1$ modulo 3, donc congru à 1 modulo 3. Donc dans tous les cas n^2 est congru à 0 ou à 1 modulo 3.

   Remarquons au passage qu'il y'a équivalence entre que n^2 est congru à 0 et n est congru à 0

   (c) Raisonnons par l'absurde et supposons qu'il existe un triplet $(x, y, z) \in \mathbb{Z}^3$ premiers entre eux dans leur ensemble tel que $x^2 + y^2 = 3z^2$ (1). Donc $x^2 + y^2 \equiv 0\ [3]$; or d'après ce qui précède, on a $\begin{cases} x^2 \equiv 0\ [3] \\ \text{ou} \\ x^2 \equiv 1\ [3] \end{cases}$ et $\begin{cases} y^2 \equiv 0\ [3] \\ \text{ou} \\ y^2 \equiv 1\ [3] \end{cases}$. Donc $\begin{cases} x^2 \equiv 0\ [3] \\ y^2 \equiv 0\ [3] \end{cases}$, donc d'après la remarque faite auparavant, $\begin{cases} x \equiv 0\ [3] \\ y \equiv 0\ [3] \end{cases}$, donc x^2 et y^2 sont multiple de 9, donc leur somme $x^2 + y^2$ aussi. Donc d'après l'égalité (1), $3z^2$ est multiple de 9, donc , donc $z^2 \equiv 0\ [3]$, donc toujours d'après la même remarque $z \equiv 0\ [3]$. Donc 3 est un diviseur commun de x, y, z ; et ceci contredit l'hypothèse qu'ils sont premiers entre eux dans leur ensemble. D'où le résultat.

   (d) Comme $M \in S_2(\mathbb{Q})$ et $\det M = -3$ et $TrM = 0$, alors $\exists\,(\alpha, \beta) \in \mathbb{Q}^2$ tel que $M = \begin{pmatrix} \alpha & \beta \\ \beta & -\alpha \end{pmatrix}$ et $\alpha^2 + \beta^2 = 3$. Soit alors $(p, q, r, s) \in \mathbb{Z} \times \mathbb{N}^* \times \mathbb{Z} \times \mathbb{N}^*$ tel que

$$\begin{cases} \alpha = \frac{p}{q} \\ \beta = \frac{r}{s} \end{cases}$$

   Donc en remplaçant dans l'égalité précédente et en multipliant par q^2s^2, il vient $p^2s^2 + r^2q^2 = 3q^2s^2$ et en divisant par d^2, où $d = p \gcd(ps, rq, qs)$, on obtient $x^2 + y^2 = 3z^2$, où $\begin{cases} x = \frac{ps}{d} \\ y = \frac{rq}{d} \\ z = \frac{qs}{d} \end{cases}$ et x, y, z sont des entiers tels que $p \gcd(x, y, z) = 1$.

   Ce qui contredie le résultat du 2c.

   On conclue donc qu'il n'existe pas de $M \in S_2(\mathbb{Q})$ dont $\sqrt{3}$ est valeur propre.

3. ..

   (a) La matrice $B = \begin{pmatrix} A & I_n \\ I_n & -A \end{pmatrix}$ répond. En effet, puisque A est à coefficients dans $\mathbb{Q}$, alors B aussi, d'autre part, comme $B^T = \begin{pmatrix} A^T & I_n \\ I_n & -A^T \end{pmatrix} = B$ puisque A est symétrique. D'autre part, par calcul matriciel par blocs, on obtient

$$B^2 = \begin{pmatrix} A^2 + I_n & 0 \\ 0 & A^2 + I_n \end{pmatrix}$$

   Or $A^2 = qI_n$, donc $B^2 = \begin{pmatrix} (q+1)\,I_n & 0 \\ 0 & (q+1)\,I_n \end{pmatrix} = (q+1)\,I_{2n}$

   (b) Raisonnons par récurrence sur d.

   * Le résultat est immédiat pour $d = 1$, il suffit de prendre $n = 1$ et $M_1 = I_1$.

   * Soit $d \geqslant 1$ et supposons l'éxistence de $n \in \mathbb{N}^*$ et des matrices $M'_1, ..., M'_d \in S_n(\mathbb{Q})$ qui commutent deux à deux telles que $M'^2_k = kI_n$ pour tout entier $1 \leqslant k \leqslant d$. Et notons $M_k = \begin{pmatrix} M'_k & 0 \\ 0 & M'_k \end{pmatrix} \in S_{2n}(\mathbb{Q})$ pour $1 \leqslant k \leqslant d$ et $M_{d+1} = \begin{pmatrix} M'_d & I_n \\ I_n & -M_d \end{pmatrix}$. Alors d'après 3a, $M_{d+1} \in S_{2n}(\mathbb{Q})$ et $M^2_{d+1} = (d+1)\,I_{2n}$. D'autre part, on vérifie que pour $1 \leqslant k \leqslant d$ les M_k commutent deux à deux puisque les M'_k commutent deux à deux et compte tenu du fait que M'_d commute avec les M'_k pour $1 \leqslant k \leqslant d$, alors par simple vérification, M_{d+1} commute avec les M_k pour tout $1 \leqslant k \leqslant d$. Donc la récurrence st achevée.

(c) Notons pour $1 \leqslant i \leqslant d$, $q_i = \frac{r_i}{s_i}$ et appliquons le résultat du 3b à l'entier $N = \max(r_1, ..., r_d, s_1, ..., s_d, d)$, alors il existe $n \in \mathbb{N}^*$ et des matrices $A_1, ..., A_N \in S_n(\mathbb{Q})$ qui commutent deux à deux et telles que $A_k^2 = kI_n$ pour $1 \leqslant k \leqslant N$. En particulier les A_k sont inversibles et $A_k^{-1} = \frac{1}{k}A_k$. On pose alors pour $1 \leqslant k \leqslant d$, $M_k = A_{r_k}.A_{s_k}^{-1}$ ou encore $M_k = \frac{1}{s_k}A_{r_k}.A_{s_k} \in \mathcal{M}_n(\mathbb{Q})$. Puisque le commutant d'une matrice est une algèbre et les A_i commutent deux à deux, alors on vérifie que les $M_k = \frac{1}{s_k}A_{r_k}.A_{s_k}$ commutent deux à deux.

D'autre part, puisque les A_i commutent deux à deux et sont symétriques, alors on montre que les $M_k = \frac{1}{s_k}A_{r_k}.A_{s_k}$ sont symétriques symétriques. Et par cmmutation des matrices A_{r_k} et A_{s_k}, on a

$$\begin{aligned} M_k^2 &= \frac{1}{s_k^2}A_{r_k}^2.A_{s_k}^2 \\ &= \frac{1}{s_k^2}(r_kI_n)(s_kI_n) \\ &= \frac{r_k}{s_k}I_n \\ &= q_kI_n \end{aligned}$$

D'où le résultat.

4. ..

(a) $\sqrt[3]{2} \notin \mathbb{Q}$. En effet, raisonnons par l'absurde et supposons $\sqrt[3]{2} \in \mathbb{Q}$ et soit $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ avec $p \wedge q = 1$, tel que $\sqrt[3]{2} = \frac{p}{q}$, donc $q\sqrt[3]{2} = p$, donc en èlevant au cube, on obtient $2q^3 = p^3$, donc q/p^3 et comme $p \wedge q = 1$, alors $p^3 \wedge q = 1$, donc $q = 1$; et en revenant à l'égalité précédente, il vient $p^3 = 2$, donc $p \in \mathbb{N}\setminus\{0, 1\}$, donc $p \geqslant 2$, donc $p^3 \geqslant 2^3 = 8 > 2$. Ce qui est absurde. Donc $\sqrt[3]{2} \notin \mathbb{Q}$. D'autre part, si $X \in E_{\sqrt[3]{2}}(M)$, alors $MX = \sqrt[3]{2}X$, donc $(M^3 - 2I_n)X = 0$, donc le polynôme $X^3 - 2$ annulle $M/E_{\sqrt[3]{2}}(M)$, donc son polynôme minimal $\pi_{M/E_{\sqrt[3]{2}}(M)}$ divise $X^3 - 2$ dans $\mathbb{Q}[X]$ (puisque M est à cefficients rationnels) ; mais $X^3 - 2$ est irréductible dans $\mathbb{Q}[X]$ puisqu'il est de degré 3 et n'a pas de racines rationnels (ses racines complexes sont $\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}$)

De plus $\pi_{M/E_{\sqrt[3]{2}}(M)}$ est unitaire de degré $\geqslant 1$,donc $\pi_{M/E_{\sqrt[3]{2}}(M)} = X^3 - 2$. Or $\pi_{M/E_{\sqrt[3]{2}}(M)}$ divise π_M et par Cayley-Hamilton π_M divise χ_M. Donc par transitivité de la divisibilité, $X^3 - 2$ divise χ_M.

(b) D'après ce qui précède, $X^3 - 2$ divise χ_M. Or comme M est symétrique réelle, alors χ_M est scindé sur $\mathbb{R}$, donc $X^3 - 2$ est aussi scindé sur $\mathbb{R}$. Ce qui est absurde, puisqu'on a vu que ses récines sont $\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}$. On conclut donc qu'il n'ya pas de matrice symétrique à coefficients dans $\mathbb{Q}$ ayant $\sqrt[3]{2}$ comme valeur propre.

5. Notons P la matrice compagne du polynôme $X^n - 1$ qui est aussi la matrice du cycle $(1, ..., n)$, c'est donc une matrice orthogonale à coefficients rationnels, dont le polynôme caractéristique est $X^n - 1$. En particulier $e^{\frac{2i\pi}{n}}$ en est une valeur propre ; et si on pose $M = \frac{1}{2}(P + P^T)$, alors $M \in \mathcal{S}_n(\mathbb{Q})$ et $\cos\left(\frac{2\pi}{n}\right)$ en est une valeur propre. en effet, soit $X \in \mathbb{C}^n\setminus\{0\}$ tel que $PX = e^{\frac{2i\pi}{n}}X$, alors $P^{-1}X = e^{-\frac{2i\pi}{n}}X$, donc $P^TX = e^{-\frac{2i\pi}{n}}X$, donc

$$\frac{1}{2}\left(P + P^T\right)X = \frac{1}{2}\left(e^{\frac{2i\pi}{n}} + e^{-\frac{2i\pi}{n}}\right)X$$

ou encore $MX = \cos\left(\frac{2\pi}{n}\right).X$, donc par passage aux conjugué et compte tenu du fait que M est à coefficients rationnels, il vient $M\overline{X} = \cos\left(\frac{2\pi}{n}\right).\overline{X}$, donc en posant $X_1 = \operatorname{Re} X$ et $X_2 = \operatorname{Im} X$, on obtient $MX_1 = \cos\left(\frac{2\pi}{n}\right).X_1$ et $MX_2 = \cos\left(\frac{2\pi}{n}\right).X_2$ et de plus $(X_1, X_2) \neq (0, 0)$ et X_1, X_2 sont dans $\mathbb{R}^n$. Donc $\cos\left(\frac{2\pi}{n}\right)$ est valeur propre de M.

6. On a

$$\begin{aligned} Q(X) &= X^d P\left(\frac{1}{X}\right) \\ &= X^d\left(\frac{1}{X^d}+\sum_{k=0}^{d-1} a_k \frac{1}{X^k}\right) \\ &= 1+\sum_{k=0}^{d-1} a_k X^{d-k} \\ &= 1+\sum_{k=0}^{d-1} a_k X^{d-k} \\ &= 1+\sum_{k=1}^{d} a_{d-j} X^j \\ &= 1+a_{d-1}X+\ldots+a_1 X^{d-1}+a_0 X^d \end{aligned}$$

D'où la première égalité.

D'autre part, $P(X)=\prod_{i=1}^{d}(X-\lambda_i)$,donc

$$\begin{aligned} Q(X) &= X^d P\left(\frac{1}{X}\right) \\ &= X^d \prod_{i=1}^{d}\left(\frac{1}{X}-\lambda_i\right) \\ &= X^d \prod_{i=1}^{d}\left(\frac{1-\lambda_i X}{X}\right) \\ &= X^d \frac{\prod_{i=1}^{d}(1-\lambda_i X)}{X^d} \\ &= \prod_{i=1}^{d}(1-\lambda_i X) \end{aligned}$$

D'où la deuxième égalitée.

7. Par simple calcul, on a pour tout $x\in\mathbb{R}$,

$$Q'(x)=\sum_{j=1}^{d}(-\lambda_j)\left(\prod_{\substack{i=1\\ i\neq j}}^{d}(1-\lambda_i X)\right)$$

donc $\forall x\in\mathbb{R}\setminus\left(\mathbb{R}\cap\left\{\frac{1}{\lambda_i}, 1\leqslant i\leqslant d\right\}\right)$,

$$\begin{aligned} f(x) &= \frac{Q'(x)}{Q(x)} \\ &= \frac{\sum_{j=1}^{d}(-\lambda_j)\left(\prod_{\substack{i=1\\ i\neq j}}^{d}(1-\lambda_i x)\right)}{\prod_{i=1}^{d}(1-\lambda_i x)} \\ &= \sum_{j=1}^{d}(-\lambda_j)\left(\frac{\prod_{\substack{i=1\\ i\neq j}}^{d}(1-\lambda_i x)}{\prod_{i=1}^{d}(1-\lambda_i x)}\right) \\ &= \sum_{j=1}^{d}-\frac{\lambda_j}{1-\lambda_j x} \end{aligned}$$

Donc $\forall x\in\mathbb{R}\setminus\left(\mathbb{R}\cap\left\{\frac{1}{\lambda_i}, 1\leqslant i\leqslant d\right\}\right)$,

$$f(x)=\sum_{j=1}^{d}-\frac{\lambda_j}{1-\lambda_j x}$$

Mais $P(0)=a_0\neq 0$, donc 0 n'est pas racine de P, donc les λ_j sont tous non nuls. Et si $j\in[[1,d]]$, alors pour tout $|x|<\frac{1}{|\lambda_j|}$, on a

$$\frac{1}{1-\lambda_j x}=\sum_{n=0}^{+\infty}(\lambda_j x)^n$$

Et en notant $r = \min\limits_{1\leqslant j\leqslant d}\left(\frac{1}{|\lambda_j|}\right)$, alors $\forall x \in]-r,r[$ et

$$\forall j \in [[1,d]], \frac{1}{1-\lambda_j x} = \sum_{n=0}^{+\infty} (\lambda_j x)^n$$

Donc $\forall x \in]-r,r[$,

$$\begin{aligned}\sum_{j=1}^{d} -\frac{\lambda_j}{1-\lambda_j x} &= -\sum_{j=1}^{d}\left(\sum_{n=0}^{+\infty}\lambda_j^{n+1}x^n\right)\\ &= -\sum_{n=0}^{+\infty}\left(\sum_{j=1}^{d}\lambda_j^{n+1}x^n\right)\\ &= -\sum_{n=0}^{+\infty}\left(\sum_{j=1}^{d}\lambda_j^{n+1}\right)x^n\\ &= -\sum_{n=0}^{+\infty} N_{n+1}x^n\end{aligned}$$

Donc $\forall x \in]-r,r[, f(x) = -\sum\limits_{n=0}^{+\infty} N_{n+1}x^n$. En particulier, on a $\forall n \in \mathbb{N}$, $N_{n+1} = -\frac{f^{(n)}(0)}{n!}$

8. ..

   (a) Si les a_i sont des rationnels, alors les polynômes Q et Q' sont à coefficients rationnels, donc la fraction rationnelle $\frac{Q'}{Q} \in \mathbb{Q}(X)$, donc toutes ses fractions dérivées successives sont dans $\mathbb{Q}(X)$, donc toutes les fonctions dérivées succéssives de $f : x \to \frac{Q'(x)}{Q(x)}$ exprimés en des rationnels, sont rationnels, en particulier, $\forall n \in \mathbb{N}$, $f^{(n)}(0) \in \mathbb{Q}$. Donc $\forall n \in \mathbb{N}, N_{n+1} = -\frac{f^{(n)}(0)}{n!} \in \mathbb{Q}$.

   (b) Supposons que $\forall n \geqslant 1, N_n \in \mathbb{Q}$. Or d'après ce qui précède, on a $\forall x \in]-r,r[$,

   $$f(x) = -\sum_{n=0}^{+\infty} N_{n+1}x^n = \frac{Q'(x)}{Q(x)}$$

   Donc

   $$\forall x \in]-r,r[, Q'(x) = \left(\sum_{n=0}^{+\infty}(-N_{n+1})x^n\right)Q(x)$$

   Or $Q(x) = \sum\limits_{k=0}^{d} a_{d-k}x^k$, et où on a posé $a_d = 1$ et $Q'(x) = \sum\limits_{k=1}^{d} k a_{d-k}x^{k-1} = \sum\limits_{n=1}^{d}(n+1)a_{d-n-1}x^n$. Donc par produit de Cauchy sur les séries entières, on a

   $$\forall x \in]-r,r[, Q(x)\sum_{n=0}^{+\infty}(-N_{n+1})x^n = \sum_{n=0}^{+\infty} c_n x^n$$

   où pour tout $n \leqslant d, c_n = \sum\limits_{k=0}^{n}(-N_{k+1})a_{d-(n-k)}$.

   Mais

   $$\forall x \in]-r,r[, Q(x)\sum_{n=0}^{+\infty}(-N_{n+1})x^n = \sum_{n=1}^{d}(n+1)a_{d-n-1}x^n$$

   Donc par unicité du développement en série entière, on a $\forall n \in [[0,d]]$,

   $$\sum_{k=0}^{n}(-N_{k+1})a_{d-(n-k)} = (n+1)a_{d-n-1}\ (*)$$

   - Cette formule (*) pour $n = 0$, donne $-N_1 = a_{d-1}$ et comme les N_i sont supposés ratyionnels, alors $a_{d-1} \in \mathbb{Q}$. soit maintenant $n \leqslant d-1$ et supposons $a_{d-1}, ..., a_{d-n}$ sont dans $\mathbb{Q}$, alors compte des rationnalités des N_i, l'élément $\sum\limits_{k=0}^{n}(-N_{k+1})a_{d-(n-k)} \in \mathbb{Q}$, donc par la formule (*), $a_{d-(n+1)} = \frac{1}{n+1}\sum\limits_{k=0}^{n}(-N_{k+1})a_{d-(n-k)} \in \mathbb{Q}$. On a donc montré par récurrence que tous les a_i sont dans $\mathbb{Q}$.

   (c) Découle de a) et b)

9. Soit $N \geqslant 1$, alors en utilisant les propriétés des sommes doubles, on a

$$\sum_{(i,j)\in[[1,n]]\times[[1,m]]}(\alpha_i\beta_j)^N = \left(\sum_{i=1}^{n}\alpha_i^N\right)\left(\sum_{j=1}^{m}\beta_j^N\right)$$

et comme A, B sont à coefficients rationnels, alors d'après le 8c, $\sum\limits_{i=1}^{n}\alpha_i^N$ et $\sum\limits_{j=1}^{m}\beta_j^N$ sont rationnels, donc leur produit aussi, donc $\sum\limits_{(i,j)\in[[1,n]]\times[[1,m]]}(\alpha_i\beta_j)^N \in \mathbb{Q}$. Donc toujours d'après le 8c, le polynôme

$\prod_{i=1}^{n}\prod_{j=1}^{m}\left(X-\alpha_i\beta_j\right)$ est à coefficients rationnels. D'autre part, en utilisant la formule du Binôme de Newton, et les propriétés des sommes doubles, on a pour tout $N \geqslant 1$, et

$$\sum_{(i,j)\in[[1,n]]\times[[1,m]]}\left(\alpha_i+\beta_j\right)^N = \sum_{(i,j)\in[[1,n]]\times[[1,m]]}\sum_{k=0}^{N} C_N^k \alpha_i^k \beta_j^{N-k}$$
$$= \sum_{k=0}^{N} C_N^k \left(\sum_{i=1}^{n}\alpha_i^k\right)\left(\sum_{j=1}^{m}\beta_j^{N-k}\right)$$

Et compte tenue de l'hypothèse A, B à coefficients rationnels et le résultat du 8c, on a pour tout $\sum_{i=1}^{n}\alpha_i^k$ est rationnel et pour tout $0 \leqslant k \leqslant N$, $\sum_{j=1}^{m}\beta_j^{N-k}$ est rationnel, donc $\sum_{k=0}^{N} C_N^k \left(\sum_{i=1}^{n}\alpha_i^k\right)\left(\sum_{j=1}^{m}\beta_j^{N-k}\right)$ est rationnel, et par suite $\sum_{(i,j)\in[[1,n]]\times[[1,m]]}\left(\alpha_i+\beta_j\right)^N \in \mathbb{Q}$. On conclut donc que le polynôme $\prod_{i=1}^{n}\prod_{j=1}^{m}\left(X-\alpha_i-\beta_j\right)$ est à coefficients rationnel.

10. Soit λ une valeur propre de M. Alors λ est racine de son polynôme caracteristique χ_M ; mais comme M est symétrique réelle, alors χ_M est scindé sur $\mathbb{R}$, donc toutes les racines de χ_M sont dans $\mathbb{R}$ et donc λ est totalement réel. Remarquons au passage que tout rationnel r est totalement réel (Prendre $P = X - r$)

11. ..

    (a) Notons $\mathcal{T}_{\mathbb{R}}$ l'ensemble des nombres totalement réel. On vérifie sans peine que $\mathcal{T}_{\mathbb{R}} \subset \mathbb{R}$ et contient 1. Soit maintenant α_1, β_1 dans $\mathcal{T}_{\mathbb{R}}$, alors quitte à diviser ses polynômes par leur coefficients dominant, on peut supposer l'existence de deux polynômes unitaires A et B à coefficients rationnels, tels que α_1 racine de A et toutes les racines de A sont dans $\mathbb{R}$ et β_1 racine de B et toutes les racines de B sont dans $\mathbb{R}$. Donc A et B s'écrivent sous la forme : $A(X) = \prod_{i=1}^{n}(X-\alpha_i)$ et $B(X) = \prod_{j=1}^{m}\left(X-\beta_j\right)$ et où les α_i et les β_j sont dans $\mathbb{R}$, alors en posant $P(X) = \prod_{i=1}^{n}\prod_{j=1}^{m}\left(X-\alpha_i\beta_j\right)$ et $Q(X) = \prod_{i=1}^{n}\prod_{j=1}^{m}\left(X-\alpha_i-\beta_j\right)$, on a d'après le 9, ces deux polynômes sont à coefficients rationnels, dont toutes les racines sont réels et $\alpha_1\beta_1$ racine de P et $\alpha_1+\beta_1$ racine de Q. Donc $\alpha_1\beta_1$ et $\alpha_1+\beta_1$ sont dans $\mathcal{T}_{\mathbb{R}}$. Donc ce dernier est stable par somme et produit. D'autre part, $\mathcal{T}_{\mathbb{R}}$ est stable par inverse, en effet soit $\lambda_1 \in \mathcal{T}_{\mathbb{R}} \setminus \{0\}$ et soit $P \in \mathbb{Q}[X]$ unitaire, ayant λ_1 pour racine et toutes ses racines sont dans $\mathbb{R}$, et notons $P = a_0 + a_1X + ... + a_{d-1}X^{d-1} + X^d$ et $\lambda_1, ..., \lambda_d$ ses racines et $Q(X)$ le polynôme réciproque de P, alors d'après le 6,

    $$Q(X) = \prod_{i=1}^{d}(1-\lambda_i X) = 1 + a_{d-1}X + ... + a_1X^{d-1} + a_0X^d$$

    En particulier $Q \in \mathbb{Q}[X]$ et $\frac{1}{\lambda_1}$ est racine de Q et toutes les racines de Q sont dans $\mathbb{R}$. Donc $\frac{1}{\lambda_1} \in \mathcal{T}_{\mathbb{R}}$. On conclut donc que ce dernier est un sous-corps de $\mathbb{R}$.

    (b) Même démarche que dans le a)

12. Notons $\alpha_1 = x$ et suppoons x totalement réel, alors il existe un polynôme A à coefficients rationnels, de la forme $A(X) = (X-\alpha_1)...(X-\alpha_d)$, avec les α_i des réels, de plus on a d'après le 8c, $\forall n \geqslant 1$, $\sum_{i=1}^{d}\alpha_i^n \in \mathbb{Q}$. Notons alors B le polynôme défini par $B(X) = \left(X-\alpha_1^2\right)...\left(X-\alpha_d^2\right)$, alors ses racines sont toutes réels positives, $\alpha_1^2 = x^2$ est racine de B, de plus $\forall n \geqslant 1$, $\sum_{i=1}^{d}\left(\alpha_i^2\right)^n = \sum_{i=1}^{d}\alpha_i^{2n} \in \mathbb{Q}$, donc toujours d'après le 8c, $B \in \mathbb{Q}[X]$. Donc x^2 est totalement positif. Réciproquement, supposons x^2 totalement positif, alors il existe un polynôme P à coefficients rationnels, de la forme $P(X) = (X-\beta_1)...\left(X-\beta_q\right)$, avec $\beta_1 = x^2$ et les β_i des réels positifs. Donc si on pose $Q(X) = P\left(X^2\right)$, on a

    $$\begin{cases} Q \in \mathbb{Q}[X] \\ Q(x) = 0 \end{cases}$$

    De plus Q est scindé sur $\mathbb{R}$ et ses racines sont $\pm\sqrt{\beta_i}$ réels. Donc x est totalement réel.

13. ..

(a) Soit $X = (x_1, ..., x_d) \in \mathbb{Q}^d$ et $X \neq 0$, alors compte tenues des propriétes de t, on a succéssivement,

$$\begin{aligned} B(X,X) &= X^T S X \\ &= \sum_{1\leqslant i,j\leqslant d} x_i x_j t\left(z^{i+j}\right) \\ &= \sum_{1\leqslant i,j\leqslant d} t\left(x_i x_j z^{i+j}\right) \\ &= \sum_{1\leqslant i,j\leqslant d} t\left(\left(x_i z^i\right)\left(x_j z^j\right)\right) \\ &= t\left(\sum_{1\leqslant i,j\leqslant d}\left(x_i z^i\right)\left(x_j z^j\right)\right) \\ &= t\left(\left(\sum_{i=1}^{d} x_i z^i\right)\left(\sum_{j=1}^{d} x_j z^j\right)\right) \\ &= t\left(\left(\sum_{i=1}^{d} x_i z^i\right)^2\right) \end{aligned}$$

Or les x_i étant des rationnels, donc totalement réels et z est supposé totalement réel, donc d'après le 11a, $\sum_{i=1}^{d} x_i z^i \in \mathcal{R}$ et donc par le 12, $x := \left(\sum_{i=1}^{d} x_i z^i\right)^2$ est totalement positif, donc d'après l'hypothèse faite sur la fonction t, $t\left(\left(\sum_{i=1}^{d} x_i z^i\right)^2\right) \geqslant 0$. D'autre part, toujours par hypothèse sur t, l'inégalité est stricte puisque $\left(\sum_{i=1}^{d} x_i z^i\right)^2 \neq 0$, en effet raisonnons par l'absurde et supposons $\left(\sum_{i=1}^{d} x_i z^i\right)^2 = 0$, donc $\sum_{i=1}^{d} x_i z^i = 0$, donc $z\left(\sum_{i=1}^{d} x_i z^{i-1}\right) = 0$ et comme z est supposé non nul, alors $\sum_{i=1}^{d} x_i z^{i-1} = 0$ ou encore $\sum_{i=0}^{d-1} x_{i+1} z^i = 0$ ou encore $P(z) = 0$ où on a posé, $P(X) = \sum_{i=0}^{d-1} x_{i+1} X^i$ et ce polynôme est à coefficients rationnels et de degré $\leqslant d-1$, ce qui contredit la minimalité de d.

Donc $\left(\sum_{i=1}^{d} x_i z^i\right)^2 \neq 0$ et par suite

$$B(X,X) = t\left(\left(\sum_{i=1}^{d} x_i z^i\right)^2\right) > 0$$

(b) Soit $X \in \ker S/\mathbb{Q}^d$, alors $X \in \mathbb{Q}^d$ et $SX = 0$, donc $X^T S X = 0$, donc d'après le 13a, $X = 0$. Donc S considéré comme endomorphisme du $\mathbb{Q}$ espace vectoriel de dimension finie $\mathbb{Q}^d$, est inversible, donc S est inversible

14. Comme S est symétrique, alors on vérifie sans peine que B est bilinéaire symétrique. De plus elle est positive, en effet soit $X = (x_1, ..., x_d) \in \mathbb{R}^d$, alors par densité de $\mathbb{Q}$ dans $\mathbb{R}$, on a pour chaque $1 \leqslant i \leqslant d$, il existe une suite $(r_{i,n})_n$ de rationnels qui converge vers x_i et notons $X_n = (r_{1,n}, ..., r_{d,n})$ de tel sorte que la suite $(X_n)_n$ converge vers X dans l'espace vectoriel normé de dimension finie $\mathbb{R}^d$. Et comme pour tout n, $X_n \in \mathbb{Q}^d$, alors d'après le 13a, $B(X_n, X_n) \geqslant 0$; mais B étant une forme bilinéaire en dimension finie, donc continue. D'où

$$B(X,X) = \lim_{n\to+\infty} B(X_n, X_n) \geqslant 0$$

On déduit alors que S est symétrique positive, de plus elle est inversible, donc (classique), elle est définie positive et donc B est définie positive. C'est donc un produit scaalaire sur $\mathbb{R}^d$.

15. ..

(a) On note $\mathcal{C} = (\varepsilon_1, ..., \varepsilon_d)$ la base canonique de $\mathbb{R}^d$, alors comme dans le procèdé de Gramm-Scmidt, mais sans normaliser (pour éviter la racine carrée), on pose $e_1 = \varepsilon_1$ et pour $2 \leqslant j \leqslant d$, $e_j = \varepsilon_j - \sum_{k=1}^{j-1} \frac{B(\varepsilon_j, e_k)}{B(e_k, e_k)} . e_k$. Mais comme S est à coefficients dans $\mathbb{Q}$, alors on vérifie que les e_i sont dans $\mathbb{Q}^d$ et d'autre part, on vérifie aussi que pour tout $i \neq j$, on a $B(e_i, e_j) = 0$. Donc $(e_1, ..., e_d)$ est une famille orthogonale de vecteurs non nuls, donc elle est libre; C'est donc une base de $\mathbb{R}^d$

(b) Notons $\mathcal{C}$ la base canonique de $\mathbb{R}^d$ et $\mathcal{B}$ la base $(e_1, ..., e_n)$ et pour $1 \leqslant i \leqslant d$, $q_i = B(e_i, e_i)$ et $D = diag(q_1, ..., q_d)$. Alors compte tenu du 15a, $D = mat(B, \mathcal{B})$ et $S = mat(B, \mathcal{C})$. Donc d'après la formule de changement de bases pour les formes bilinéaires, $S = P^T D.P$, avec P la matrice de passage de la base $\mathcal{C}$ à la base $\mathcal{B}$ qui est inversible à coefficients rationnels puisque les $e_i \in \mathbb{Q}^d$.

16. On reconnait la matrice compagne du polynôme $Z(X)$. Donc (c'est classique) son polynôme caractéristique est $Z(X)$

17. ..

(a) Notons $E_1, ..., E_d$ la base canonique de $\mathbb{R}^d = M_{d,1}(\mathbb{R})$, alors la famille des colonnes de M dans l'ordre, est

$$(E_2, ..., E_d, (a_0, ..., a_{d-1}))$$

D'autre part, pour $1 \leqslant i, j \leqslant d$, le coefficient $(SM)_{i,j}$ se trouvant dans la $i^{ème}$ ligne et $j^{ème}$ colonne de SM est le produit

$$\begin{cases} \left(t\left(z^{i+1}\right), ..., t\left(z^{i+j}\right), ..., t\left(z^{i+d}\right)\right) E_{j+1} \text{ si } j \neq d \\ \left(t\left(z^{i+1}\right), ..., t\left(z^{i+j}\right), ..., t\left(z^{i+d}\right)\right) \begin{pmatrix} a_0 \\ \vdots \\ a_{d-1} \end{pmatrix} \text{ si } j = d \end{cases}$$

ou encore

$$(SM)_{i,j} = \begin{cases} t\left(z^{i+j+1}\right) \text{ si } j \neq d \\ \sum_{k=0}^{d-1} a_k t\left(z^{i+k+1}\right) \end{cases}$$

Mais, compte tenue de la rationnalité des a_i et par hypothèse faite sur la fonction t, on a

$$\begin{aligned} \sum_{k=0}^{d-1} a_k t\left(z^{i+k+1}\right) &= t\left(\sum_{k=0}^{d-1} a_k z^{i+k+1}\right) \\ &= t\left(z^{i+1} \sum_{k=0}^{d-1} a_k z^k\right) \\ &= t\left(z^{i+1} \sum_{k=0}^{d-1} a_k z^k\right) \\ &= t\left(z^{i+1}\left(z^d - Z(z)\right)\right) \\ &= t\left(z^{i+1+d}\right) \text{ car } Z(z) = 0 \end{aligned}$$

On a donc

$$(SM)_{i,j} = \begin{cases} t\left(z^{i+j+1}\right) \text{ si } j \neq d \\ t\left(z^{i+1+d}\right) \text{ si } j = d \end{cases}$$

Ce qui prouve donc que SM est symétriue.

(b) On a $SM = P^T DPM$ et $(SM)^T = M^T S^T = M^T P^T DP$; et comme SM ests ymétrique, alors $\left(P^T DP\right) M = M^T \left(P^T DP\right)$. Or $P^T DP = P^T \Delta.\Delta P$ où on a posé $\Delta = diag\left(\sqrt{q_1}, ..., \sqrt{q_d}\right)$. Et compte tenue de la symétrie de la matrice diagonale,

$$\begin{aligned} P^T \Delta.\Delta P &= (\Delta P)^T (\Delta P) \\ &= R^T R \end{aligned}$$

Donc $R^T RM = M^T R^T R$ et en composant à gauche par $\left(R^T\right)^{-1}$ puis par R^{-1} à droite, on obtient $RMR^{-1} = \left(R^T\right)^{-1} M^T R^T$. Mais $\left(R^T\right)^{-1} = \left(R^{-1}\right)^T$. Donc $RMR^{-1} = \left(R^{-1}\right)^T M^T R^T = \left(RMR^{-1}\right)^T$. D'où RMR^{-1}est symétrique.

18. On conserve les notations précédentes : $\Delta = diag\left(\sqrt{q_1}, ..., \sqrt{q_d}\right)$ et $D = \Delta^2$. On a d'après le résultat du 3c, il existe $n \in \mathbb{N}^*$ et des matrices $M_1, ..., M_d$ dans $S_n(\mathbb{Q})$ qui commutent deux à deux et telles que pour tout $1 \leqslant i \leqslant d$, $M_i^2 = q_i I_n$. En particulier les M_i sont inversibles. Notons aussi $A = \Delta\left(RMR^{-1}\right)\Delta$, alors A est symétrique puisque Δ est symétrique car diagonale et RMR^{-1} est symétrique d'après le 17b ; d'autre part,

comme $R = \Delta P$, alors $A = \Delta\left(\Delta PMP^{-1}\Delta^{-1}\right)\Delta = \Delta^2 PMP^{-1}$. Mais $\Delta^2 = D$, P et M sont à coefficients dans $\mathbb{Q}$, donc P^{-1} aussi et donc leur produit $\Delta^2 PMP^{-1}$ aussi, par suite $A \in S_d(\mathbb{Q})$. D'autre part, si on note $\Lambda = diag\left(\underbrace{D,...,D}_{n \text{ fois}}\right)$, alors il existe une matrice de permutations Q (donc à coefficients dans $\mathbb{Q}$), telle que $Q^{-1}\Lambda Q = diag\left(q_1 I_n,...,q_d I_n\right)$ ou encore puisque Q est orthogonale,

$$\begin{aligned} Q^T\Lambda Q &= diag\left(q_1 I_n,...,q_d I_n\right) \\ &= diag\left(M_1^2,...,M_d^2\right) \\ &= \left(diag\left(M_1,...,M_d\right)\right)^2 \\ &= N^2 \quad (1) \end{aligned}$$

avec $N = diag\left(M_1,...,M_d\right)$ qui est symétrique inversible à coefficients dans $\mathbb{Q}$ et donc son inverse aussi, puisque les M_i le sont. Et en posant $B = diag\left(\underbrace{A,...,A}_{n \text{ fois}}\right)$ qui est aussi symétrique à coefficients dans $\mathbb{Q}$ ainsi que son inverse, puisque D l'est, alors la matrice $C = N^{-1}Q^T BQN^{-1}$ répond à la question. En effet, elle à coefficients dans $\mathbb{Q}$, car produit de matrices à coefficients dans $\mathbb{Q}$ et comme N^{-1} et B sont symétriques, alors en prenant sa transposé, on vérifie que C est aussi symétrique. D'autre part,

$$\begin{aligned} C &= N^{-1}Q^T BQN^{-1} \\ &= N^{-1}\left(Q^T BQ\right)N^{-1} \\ &= N^{-1}\left(Q^T BQ\right)N^{-1} \end{aligned}$$

or

$$\begin{aligned} B &= diag\left(\underbrace{A,...,A}_{n \text{ fois}}\right) \\ &= diag\left(\underbrace{\Delta^2 PMP^{-1},...,\Delta^2 PMP^{-1}}_{n \text{ fois}}\right) \\ &= diag\left(\underbrace{\Delta^2,...,\Delta^2}_{n \text{ fois}}\right) diag\left(\underbrace{PMP^{-1},...,PMP^{-1}}_{n \text{ fois}}\right) \\ &= \Lambda diag\left(\underbrace{PMP^{-1},...,PMP^{-1}}_{n \text{ fois}}\right) \\ &= \Lambda M' \end{aligned}$$

avec

$$M' = diag\left(\underbrace{PMP^{-1},...,PMP^{-1}}_{n \text{ fois}}\right)$$

Donc

$$\begin{aligned} C &= N^{-1}\left(Q^T\Lambda M'Q\right)N^{-1} \\ &= N^{-1}\left(Q^T\Lambda QQ^T M'Q\right)N^{-1} \text{ car } Q \text{ orthogonale} \\ &= N^{-1}\left(N^2 Q^T M'Q\right)N^{-1} \text{ d'après l'=(1)} \\ &= NQ^T M'QN^{-1} \\ &= \left(QN^{-1}\right)^{-1} M'\left(QN^{-1}\right) \end{aligned}$$

Donc C est semblable à

$$M' = diag\left(\underbrace{PMP^{-1},...,PMP^{-1}}_{n \text{ fois}}\right)$$

dont le polynôme caractéristique est $\chi_M^n = Z^n$. Or z est racine de Z, donc z est valeur propre de C.